Datenschutz-Folgenabschätzung (DSFA) gem. Art. 35 DSGVO

Verantwortliche Stelle: _____

Auftragsverarbeiterin: **No Isolation GmbH**

Verarbeitung: **AV1 Telepräsenzroboter**

Dokumenten-Historie

Version	Datum	Bearbeiter	Bearbeitung
1.0	25.05.2023	Blechschmidt, msecure GmbH	Erstellung / Initialisierung
1.1	01.09.2023	Mainka, msecure GmbH	Übersetzung ins Deutsche, Überarbeitung und Ergänzung von Angaben insb. zum Angemessenheitsbeschluss DPF der Kommission (Art. 45 DSGVO)

Beurteilung der Notwendigkeit einer Datenschutz-Folgenabschätzung

Fassen Sie zusammen, warum Sie die Notwendigkeit einer Datenschutzfolgenabschätzung festgestellt haben:

☐ Evaluation oder Scoring

☐ Automatisierte Entscheidungsfindung mit rechtlicher oder ähnlicher Signifikanz

☐ Systematische Überwachung

☐ Sensible Daten oder Daten höchstpersönlicher Natur

☐ Datenverarbeitung in großem Ausmaß

☐ Abgleich oder Kombination von Datensätzen

☒ Datenverarbeitung besonders schützenswerter Personengruppen

☒ Innovative Anwendung oder Einführung neuer technologischer oder organisatorischer Lösungen

☐ Datenverarbeitung verhindert Wahrnehmung von Rechten betroffener Personen oder Vertragspflichten

☐ Systematische Überwachung öffentlicher Bereiche

☐ Verarbeitung ist auf der Blacklist einer Aufsichtsbehörde

Nächster Prüfungstermin

01.09.2024

Inhaltsverzeichnis

1 Inhalt

1 Erfüllung der rechtlichen Anforderungen nach DSGVO

Prüfkriterium	Anmerkung	Erfüllt
Grundsätze und Rechtmäßigkeit der Verarbeitung	Die Verarbeitung erfolgt auf der Grundlage von Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO; sie kann auch auf anwendbare Schulgesetze gestützt werden, soweit vorhanden. Die Bedingungen für die informierte und freiwillige Einwilligung gem. Art. 7 DSGVO werden eingehalten	☐
Maßnahmen im Sinne der Rechte der Betroffenen	No Isolation ist vertraglich verpflichtet, den für die Verarbeitung Verantwortlichen bei der Erfüllung der Rechte der betroffenen Personen zu unterstützen (AV-Vertrag §14). Das Auskunftsrecht wird durch die Datenschutzinformationen auf der Website unterstützt. Die Datenlöschung ist vertraglich vereinbart und technisch abgesichert.	☐
Grundlage der Auftragsverarbeitung	Mit No Isolation wurde eine Datenverarbeitungsvereinbarung (AV-Vertrag gem. Art. 28 DSGVO) einschließlich der EU-SCC zum Zweck der Verarbeitung der für die Erbringung der Dienstleistung erforderlichen personenbezogenen Daten geschlossen. Der Einsatz von Unterauftragsverarbeitern durch No Isolation unterliegt den Bestimmungen des AVV.	☐
Bewertung der Risiken für die Datenverarbeitung unter Berücksichtigung der TOM nach Art. 25, 32 DSGVO	Die von No Isolation und AWS beschriebenen und durch Zertifikate glaubhaft gemachten technischen und organisatorischen Maßnahmen entsprechen dem Stand der Technik und sind für die Datenverarbeitung mit AV1 geeignet.	☐
Dringend empfohlene Maßnahmen	Überprüfung und Harmonisierung der bereitgestellten Datenschutzerklärung (englische vs. deutsche Version). Erwägung der Benennung eines Datenschutzbeauftragten. Erwägung der Verwaltung von Verschlüsselungsschlüsseln außerhalb der US-Clouds.	

2 Ergebnis der Datenschutz-Folgenabschätzung und Empfehlung

Die Durchführung der DSFA, einschließlich der Risikoanalyse,

☒ erfolgte korrekt. Die festgelegten Maßnahmen entsprechen im Verhältnis den Risiken der Betroffenen. Die DSFA verlief positiv.
Empfehlung: Nutzung der Verarbeitungstätigkeit

☐ erfolgte korrekt. Die festgelegten Maßnahmen entsprechen im Verhältnis **nicht** den Risiken der Betroffenen und sind **nicht** ausreichend.
Eine Nach-Folgenabschätzung und erneute Maßnahmenfestlegung sind notwendig.

☐ erfolgte unkorrekt. Die festgelegten Maßnahmen entsprechen im Verhältnis den Risiken der Betroffenen und sind ausreichend.
Eine erneute Betrachtung mit einhergehender Nach-Folgenabschätzung ist notwendig.

☐ erfolgte unkorrekt. Die festgelegten Maßnahmen entsprechen im Verhältnis **nicht** den Risiken der Betroffenen und sind **nicht** ausreichend. Weitere Maßnahmen sind ausgeschlossen. Die DSFA verlief negativ.
Empfehlung: Konsultation Aufsichtsbehörde

3 Stammdaten des Unternehmens / der Organisation

3.1 Namen und Kontaktdaten des Verantwortlichen

Name / Bezeichnung der datenverarbeitenden Stelle	[Daten der Bildungseinrichtung]
Straße und Hausnummer	
PLZ und Ort	
Telefon	
Telefax	
E-Mail-Adresse	
Internet-Adresse	

3.2 Persönliche Nennung der verantwortlichen Personen

Geschäftsführung	
Vollständiger Name	
Telefon	
E-Mail-Adresse	
Leitung der Datenverarbeitung	
Vollständiger Name	
Telefon	
E-Mail-Adresse	
Datenschutzbeauftragte/r	
Vollständiger Name	
Telefon	
E-Mail-Adresse	

3.3 Name und Kontaktdaten der Auftragsverarbeiterin	
Name / Bezeichnung der datenverarbeitenden Stelle	No Isolation GmbH
Straße und Hausnummer	Viktualienmarkt 8
PLZ und Ort	80331 München
Telefon	+49 (0)89 3803 4115
Telefax	
E-Mail-Adresse	de@noisolation.com
Internet-Adresse	www.noisolation.com/de

3.4 Persönliche Nennung der verantwortlichen Personen (No Isolation)	
Geschäftsführung	
Vollständiger Name	Hans Fredrik Vestneshagen
Telefon	+47 23 96 58 30
E-Mail-Adresse	vestneshagen@noisolation.com
IT Management	
Vollständiger Name	Frode Hansen
Telefon	+47 23 96 58 30
E-Mail-Adresse	hansen@noisolation.com

4 Allgemeiner Überblick der Datenverarbeitungen

4.1 Beschreibung der Verarbeitungstätigkeit

Benennen Sie die Verarbeitung und erläutern Sie in groben Zügen, was mit dem Projekt erreicht werden soll und welche Arten der Bearbeitung es umfasst. Es kann hilfreich sein, auf andere Dokumente, wie z.B. eine Projektskizze oder eine Projektbeschreibung, zu verweisen oder zu verlinken:

Der AV1-Telepräsenzroboter ist ein Werkzeug, das die Integration von Schülern erleichtert, die über einen längeren Zeitraum nicht am Unterricht teilnehmen können. Die Lösung AV1 ist so konzipiert, dass der Schüler das Geschehen im Unterricht von zu Hause aus verfolgen kann (Audio und Video). Gleichzeitig soll er es den Mitschülern und Lehrern im Klassenzimmer ermöglichen, die Signale und Beiträge des Schülers (Audio) wahrzunehmen.

4.2 Zwecke der Verarbeitung

Beschreiben Sie die Zwecke der Verarbeitung: Was wollen Sie erreichen? Was ist die beabsichtigte Wirkung auf Personen? Was sind die Vorteile der Verarbeitung - für Sie und im Allgemeinen?

Grundlegendes Ziel ist es, bei längerer Abwesenheit die aktive Teilnahme am Unterricht und die Integration in die Klassengemeinschaft zu ermöglichen und einen Lernrückstand des betroffenen Schülers zu verhindern.

Besondere Zwecke im Rahmen der Datenverarbeitung sind:

4.2.1 Bereitstellung von AV1 und AV1-Assistant App

- Ermöglichung des Einsatzes und der Nutzung von AV1 zum Zwecke des Live-Video-Streamings,

- die Verwaltung und das Management der relevanten Dienste, einschließlich des Onboarding von Kunden,

- Erstellung und Verwaltung von Kundenkonten und Authentifizierung von Kundenbenutzern

- Verwaltung des AV1-Bestands (z. B. Generierung von Schlüsselwörtern für neue Benutzer; Erstellung einer AV1-Assetliste)

- Versorgung des Kunden mit statistischen und anderen Informationen über die Nutzung der Dienste

- Verfolgen, wann AV1 aktiviert ist; Verfolgen der Nutzung von AV1 nach der Aktivierung

- Implementierung von Sicherheitsmaßnahmen und Problemlösung

4.2.2 Bereitstellung von technischem Support sowohl für Kunden als auch für Endbenutzer (einschließlich Untersuchung von Support-Problemen und Fehlerbehebung)

4.3 Begleitende Unterlagen

☐ Risikobewertung
☒ Verzeichnis der Verarbeitungstätigkeit
☒ Auftragsverarbeitungsvertrag
☒ Datenstrom-Diagramm
☐ Löschkonzept
☐ Backupkonzept
☐ Kryptographiekonzept
☐ Berechtigungskonzept / Rollenkonzept
☐ Datenschutzkonzept bzw. Datenschutzrichtlinie
☐ IT-Sicherheitskonzept
☒ Übersicht der Technischen und Organisatorischen Maßnahmen (TOMs)

Weitere Dokumentation und Unterlagen:

- AV1 - Description of processing (December 2022)
- AV1 Technical and organisational security measures
- AV1 Informationen zum Datenschutz 11.08.23
- AV-Vertrag Deutsch – Stand 06.07.2023
- No Isolation Sub-processors
- Anlage 2_Einleitendes Informationsschreiben an Erziehungsberechtigte_15.12.21
- Anlage 2b_Einwilligungserklärung Erziehungsberechtigte_15.12.21
- Anlage 3b_Einwilligungserklärung Lehrkräfte_15.12.21

4.4 Beschreibung des Verarbeitungsverfahrens

Beschreiben Sie die Art der Verarbeitung: Wie werden Sie Daten erheben, verwenden, speichern und löschen? Es könnte sich als nützlich erweisen, ein Flussdiagramm oder eine andere Art der Beschreibung von Datenflüssen heranzuziehen.

Die Lösung besteht aus dem AV1-Hardwaregerät ("Avatar") und der AV1-App ("AV1 App") auf dem Gerät des Nutzers. Personenbezogene Daten werden vom "Kundennutzer" (d. h. Mitarbeiter der Bildungseinrichtung, die zur Nutzung des Dienstes berechtigt sind) und "Endnutzer" (d. h. Schüler, die die AV1-App nutzen, oder deren Eltern) erhoben. No Isolation agiert als Dienstleister für die Bildungseinrichtung und/oder den Käufer, der die Lösung implementiert.

Der abwesende Schüler nutzt die AV1-App, um zu sehen und zu hören, was im Klassenzimmer passiert. Dazu wird ein Videostream zwischen dem AV1-Avatar und der AV1-App aufgebaut. Audio und Wortmeldungen werden von der App des Schülers übertragen, aber kein Video.

Sobald die Verbindung hergestellt ist, werden die Videodaten von den No Isolation-Servern nur für die Zeit der Übertragung verarbeitet (live, keine Aufzeichnung, nur flüchtiger Speicher). Statistische Daten über die Nutzung von AV1 werden auf No Isolation-Servern gespeichert und dem Kunden auf Anfrage zur Verfügung gestellt.

Beschreiben Sie den Kontext der Verarbeitung: *Welche Art von Beziehung besteht zwischen Ihnen und den betroffenen Personen? Handelt es sich um Kinder oder andere schutzbedürftige Gruppen? Gab es in der Vergangenheit Bedenken hinsichtlich dieser Art der Verarbeitung oder Sicherheitsmängel? Ist sie in irgendeiner Weise neu?*

Bei den Nutzern handelt es sich entweder um Schüler, die unter 16 Jahre alt sein können, oder um Lehrer und Verwaltungspersonal der Bildungseinrichtung. Die Anwendung kann als eine innovative Lösung für die Fernteilnahme am Unterricht betrachtet werden. Die Video- und Audioübertragungen aus den Klassenräumen können durch mündliche Äußerungen Hinweise auf den Gesundheitszustand, religiöse Überzeugungen und andere besondere Datenkategorien geben. Diese Informationen werden nur vorübergehend für die Dauer der Übertragung verarbeitet.

Videostreams und gespeicherte Daten werden durch Verschlüsselung geschützt. Allerdings ist es aus technischen Gründen unvermeidbar, dass IP-Adressen während der Videoübertragung unverschlüsselt im Kurzzeitspeicher des Servers verbleiben.

4.5 Kategorien von personenbezogenen Daten

Beschreiben Sie den Umfang der Verarbeitung: *Wie viele Daten werden Sie sammeln und verwenden? Wie oft? Wie lange werden Sie sie aufbewahren? Wie viele Personen sind betroffen?*

Die personenbezogenen Daten von Kundennutzern und Endnutzern werden einmalig zur Einrichtung der Benutzerkonten erhoben. Videodaten werden nur für die Dauer der Übertragung verarbeitet. Eine Aufzeichnung ist nicht möglich; die Erstellung von Bildschirmfotos wird verhindert. Statistische Daten werden dem Avatar in der Schule und dem Gerät des Endnutzers zugeordnet (pseudonymisierte ID); für den Dienstleister No Isolation ist es grundsätzlich nicht möglich, den Endnutzer als natürliche Person zu identifizieren. Die Daten werden in der Regel innerhalb von 6 Monaten nach Beendigung des Vertragsverhältnisses gelöscht.

Um welche Art von Daten handelt es sich, und gehören dazu besondere Kategorien von Daten oder Daten über Straftaten (Art. 9 und 10 DSGVO)?

Datenarten	Datenkategorien
☒ Allgemeine personenbezogene Daten	• Identität, Identifikationsdaten • Berufliches Leben (Lebenslauf, Schul- und Berufsausbildung, Auszeichnungen, usw.) • Verbindungsdaten (IP-Adressen, Ereignisprotokolle, etc.)
☐ Sensible personenbezogene Daten	• Sozialversicherungsnummer • Bankdaten
☒ Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) *	• Philosophische, politische, religiöse und gewerkschaftliche Ansichten, Sexualleben, Gesundheitsdaten, rassische oder ethnische Herkunft, Daten über Gesundheit oder Sexualleben, biometrische Daten
☐ Daten über strafrechtliche Verurteilungen und	• Daten über Straftaten, Verurteilungen, Sicherungsmaßnahmen

Straftaten (Art. 10 DSGVVO)	
☐ Daten zur Erstellung oder Nutzung von automatisierten persönlichen Profildateien	• Leistung am Arbeitsplatz • Wirtschaftliche Lage • Gesundheit • Persönliche Vorlieben oder Interessen • Verlässlichkeit oder Verhalten • Standort oder Bewegungen
☒ Personenbezogene Daten besonders schutzbedürftiger Personengruppen (z. B. Kinder)	• Video- und Audiodaten (Mitschüler) • Audiodaten (abwesender Schüler/Endbenutzer)

***) Anmerkung: Besondere Datenkategorien können nur aus der Beobachtung des Live-Streams im Zusammenhang mit Klassenveranstaltungen entnommen werden (nicht-persistente Daten)**

Herkunft der Daten	**Detaildarstellung**
☐ Mitarbeiter ☐ Lieferanten ☐ Kunden ☒ Mitarbeiter des für die Verarbeitung Verantwortlichen ☒ Daten von dritten Personen ☒ Nutzungsbezogene Daten (Metadaten)	- Berechtigungsnachweise und Authentifizierungsdaten von Mitarbeitern von Kunden und Endnutzern. - IP-Adressen von NAT-Geräten (Heimrouter des Endnutzers, Router der Bildungseinrichtung) - Audio-/Videodaten von Mitschülern, Lehrern - Audiodaten des abwesenden Schülers (Endnutzer) - Name und Kontaktdaten der Mitarbeiter des Verantwortlichen - Metadaten (Länge und Qualität der Videoübertragung, Datum und Uhrzeit, Informationen zum drahtlosen Netzwerk, Verbindungsstärke, Informationen zum Mobilfunknetz)

4.6 Kategorien von Empfängern

Werden Daten an Dritte übermittelt oder mit diesen geteilt?

Empfänger	**Datenkategorien**	**Zweck**	**Drittlandstransfer?**
Amazon Web Services EMEA SARL, 38 Av. John F. Kennedy, 1855, Luxembourg	Identifikationsdaten, (Konten), IP-Adressen, Videostreamdaten, Nutzungsdaten, Protokolle	AWS ist der IaaS-Cloud-Anbieter für No Isolation, (Dienste: CloudWatch, EC2, EKS, Kinesis, RDS, VPC, Elastic Load Balancing, DocumentDB)	Möglich*

HubSpot Ireland Ltd, Ground Floor, Two Dockland Central, Guild Street, Dublin 1, Co. Dublin, Irland	Kontaktdaten	Live-Chat und E-Mail-Dienste zur Unterstützung von Kunden- und Endnutzern	Möglich*
No Isolation AS, Trondheimsveien, 2, 0560 Oslo, Norwegen	Kontaktdaten, Nutzungsdaten	Unterstützung von Kundennutzern und Endnutzern bei Anfragen zu den Diensten.	EWR
No Isolation Ltd., 239 Old St, London, EC1V 9EY, United Kingdom	Kontaktdaten, Nutzungsdaten	Unterstützung von Kundennutzern und Endnutzern bei Anfragen zu den Diensten.	Ja, Angemessenheits beschluss gem. Art. 45 DSGVO für UK

*) Datenübermittlung in die USA: Die gekennzeichneten Unterauftragsverarbeiter haben eine Niederlassung in der EU und gewährleisten, dass die Verarbeitung auf Servern in der EU erfolgt. Eine Übermittlung von Daten in die USA findet daher nur statt, wenn Daten bestimmter Personen auf richterliche Anordnung zur Verfolgung von Straftaten oder zur Abwehr terroristischer Bedrohungen herausgegeben werden müssen.

Der Auftragsverarbeiter hat mit jedem Unterauftragsverarbeiter Verträge nach den geltenden EU-Standards (EU SCC) abgeschlossen. Alle Unterauftragsverarbeiter haben zusätzliche Garantien festgelegt, um die Auswirkungen einer möglichen Datenübermittlung an US-Behörden zu minimieren, wie z. B. die Inanspruchnahme des Rechtsweges im Falle von Anfragen. Aufgrund des bestehenden Konflikts der Rechtssysteme in den USA und der EU kann ein solcher Datenzugriff nicht völlig ausgeschlossen werden. Die Wahrscheinlichkeit eines tatsächlichen Datenzugriffs erscheint vor dem Hintergrund, dass die Daten in den Plattformen entweder nicht personalisiert, nicht persistent oder risikoarm sind, sehr gering.

Für Datenübermittlungen in die USA haben sich die Anbieter dem EU-US-Datenschutzrahmen (EU-US Data Privacy Framework) angeschlossen, der auf Basis eines Angemessenheitsbeschlusses der Europäischen Kommission gemäß Art. 45 DSGVO die Datenübertragung legitimiert.

5 Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge (in Bezug zu ihrem Zweck)

5.1 Grundsätze und Rechtmäßigkeit der Verarbeitung

Rechtmäßigkeit, Treu und Glauben, Transparenz der Verarbeitung (Art. 5 Abs. 1 lit. a DSGVO)	Die Verarbeitung personenbezogener Daten basiert auf Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO. Von allen Beteiligten werden Einwilligungserklärungen eingeholt, die mit einer ausreichenden Vorabinformation verbunden sind. Zu diesem Zweck stellt No Isolation dem Verantwortlichen vorgefertigte Dokumente zur Verfügung.
Festgelegte, eindeutige und legitime Zwecke (Art. 5 Abs. 1 lit. b DSGVO)	Die Verarbeitung erfolgt, um eine Plattform für die Einbindung abwesender Schüler in den Unterricht bereitzustellen. Die damit verbundenen Zwecke der Bereitstellung der Plattform, der Verwaltung von Geräten und Konten, der Nutzungsanalyse und der Sicherheitsverfahren erscheinen für diesen Zweck legitim. Die verwendeten Daten sind notwendig, um die angegebenen Zwecke zu erfüllen.
Angaben zur Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO)	Es werden verschiedene Maßnahmen ergriffen, um die Identifizierbarkeit von Einzelpersonen durch den Auftragsverarbeiter auf das notwendige Maß zu beschränken. So hat der Auftragsverarbeiter beispielsweise keine Kenntnis von der Identität der Nutzer, da die Erkennung hauptsächlich auf Identifikatoren (Seriennummern des Avatars) oder pseudonymisierten IDs basiert, die von dem für die Verarbeitung Verantwortlichen generiert werden
Angaben zur Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO)	Die Speicherung der Daten ist grundsätzlich auf die vertragliche Nutzungsdauer von AV1 beschränkt. Darüber hinaus kann jederzeit auf Wunsch eine Löschung der gespeicherten personenbezogenen Daten erwirkt werden. Videodaten werden nur für die Dauer der Verbindung bereitgestellt und somit für die minimal mögliche Dauer verarbeitet.
Angaben zu Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f DSGVO)	Die Auswahl der AWS-Plattform als einer der Hyperscaler garantiert die Erfüllung modernster Integritätsanforderungen. Zur Gewährleistung der Vertraulichkeit, z. B. gegen Cyberangriffe, sind verschiedene Sicherheitsmechanismen im Einsatz. Die Lösung basiert auf einer weitgehenden Anonymität der Endnutzer für den Dienstleister und seine Subauftragnehmer.

5.2 Maßnahmen im Sinne der Rechte der Betroffenen	
Auskunftsrecht und Recht auf Datenübertragbarkeit (Art. 15 und Art. 20 DSGVO)	Die betroffenen Personen oder der Träger der elterlichen Verantwortung werden schriftlich über die Rechte der betroffenen Person und insbesondere über das Recht auf Auskunft und das Recht auf Datenübertragbarkeit informiert. Die Datenschutzerklärung des Auftragsverarbeiters ist auf der Website und über die App-Einstellungen leicht zugänglich.
Recht auf Berichtigung und Löschung (Art. 16 und Art. 17 DSGVO)	Alle betroffenen Personen (Endnutzer, Kundennutzer, Mitschüler oder deren Eltern) werden vor der Nutzung von AV1 schriftlich über die Rechte der Betroffenen und insbesondere über das Recht auf Berichtigung und Löschung informiert.
Widerspruchsrecht und Recht auf Einschränkung der Verar-beitung (Art. 21 und Art. 18 DSGVO)	Die betroffenen Personen oder der Träger der elterlichen Verantwortung werden schriftlich über die Rechte der betroffenen Person und insbesondere über das Widerspruchsrecht und das Recht auf Einschränkung der Verarbeitung informiert.
Recht auf Beschwerde bei einer Aufsichtsbehörde (Art. 77 DSGVO)	Alle betroffenen Personen werden schriftlich über das Recht zur Beschwerde bei einer Aufsichtsbehörde informiert.

6 Erfüllung der Anforderungen an die Sicherheit der Datenverarbeitung nach Art. 25, 32 DSGVO

6.1 Bewertung der umgesetzten technischen und organisatorischen Maßnahmen (TOM) zur Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit

Maßnahmen zur **Pseudonymisierung, Verschlüsselung** oder **Anonymisierung** personenbezogener Daten	☒ Pseudonymisierung Der Endnutzer erhält eine pseudonymisierte Benutzerkennung durch den Verantwortlichen. Der Dienstleister No Isolation erhält keine Kenntnis über die Identität des Nutzers. ☒ Verschlüsselung ☒ Transportdatenverschlüsselung ☒ Verschlüsselung ruhender Daten ☐ Die Verschlüsselungsschlüssel werden ausschließlich von dem für die Verarbeitung Verantwortlichen verwaltet (bei Cloud-Lösungen in Drittländern, z. B. den USA) Die Verschlüsselung erfolgt mit TLS 1.2 und AES256-bit ☒ Anonymisierung Alle Metadaten werden anonymisiert, wenn es kein aktives Abonnement für AV1 mehr gibt.
Maßnahmen zur Gewährleistung der **Vertraulichkeit** der Systeme und Dienste bei der Verarbeitung	☒ Physische Zutrittskontrolle Alle Räumlichkeiten sind mit Einbruchmeldeanlagen und Videoüberwachung an den Ein- und Ausgängen ausgestattet, die von den Vermietern verwaltet und gewartet werden. Es werden Maßnahmen ergriffen, um zu verhindern, dass sich Unbefugte Zugang zu den Räumlichkeiten verschaffen, in denen sich die Systeme befinden. Das Personal von No Isolation ist in den Verfahren zum sicheren Ver- und Entriegeln der Räumlichkeiten geschult. Das Personal von No Isolation muss individuelle PIN-geschützte Schlüsselkarten oder herkömmliche physische Schlüssel (je nach Standort) verwenden, um Zugang zu den Räumlichkeiten zu erhalten. Das Personal mit Schlüssel ist in der Ausrüstungsliste aufgeführt, die vom Büroleiter in Norwegen geführt und an die Direktoren in Deutschland und im Vereinigten Königreich delegiert wird. Besucher von Gebäuden müssen jederzeit von No Isolation-Personal begleitet werden.

	☒ Zugangskontrolle (administrative / organisat. Kontrolle) Nur befugte Personen haben Zugang zu Systemen, in denen personenbezogene Daten und Metadaten gespeichert sind. Der Zugang zu den Systemen wird auf einer Need-to-know-Basis gewährt und wird überwacht und protokolliert. Die internen und kundeneigenen Verwaltungssysteme von No Isolation verwenden rollenbasierte Zugriffskontrollen, die die Fähigkeit zur Änderung oder Löschung von Daten auf bestimmte Kundenorganisationen und autorisierte Benutzergruppen beschränken. Der Zugriff auf Systeme und Cloud-basierte Konten basiert auf einer zugewiesenen Benutzer-ID und einer Zwei-Faktor-Authentifizierung. Der Zugriff auf die Infrastruktur von No Isolation unterliegt Sicherheitsregeln und -vorschriften, die nur Datenverkehr von autorisierten Quellen zulassen. Der Zugang zu den Ressourcen der Infrastruktur ist auf No Isolation-Administratoren (Betriebspersonal) beschränkt, die den Zugang benötigen, um Wartungsarbeiten an den Systemen durchzuführen.
Maßnahmen zur Gewährleistung der **Integrität** der Systeme und Dienste bei der Verarbeitung	**Ereignisprotokollierung** (z.B. bei der Nutzerauthentifizierung oder Dateneingabe, -veränderung oder -löschung): ☒ ***Eingabekontrolle*** *(Überprüfung, zu welcher Zeit und von wem personenbezogener Daten eingegeben, verändert oder gelöscht wurden)* Die Systeme sind nur einem minimalen Satz von Endpunkten ausgesetzt, die für die Bereitstellung von Diensten erforderlich sind. Die offenen Endpunkte unterstützen nur HTTPS und alle Clients müssen sich gegenüber dem System authentifizieren, bevor die Endpunkte genutzt werden können. Es werden Maßnahmen ergriffen, um zu überprüfen, wer persönliche Daten in die Systeme eingegeben, geändert oder entfernt hat. Datenbank- und Datenspeichersysteme werden durch kontinuierliche Anwendung von Wartungsmaßnahmen, Empfehlungen und Best Practices der Anbieter gewartet; alle Verfahren, mit denen personenbezogene Daten eingegeben, gespeichert und bearbeitet werden, sind mit eingebauten Integritäts- und Sicherheitsvorkehrungen konzipiert. Alle diese Verfahren werden vor ihrer Implementierung gründlich getestet und von Fachleuten begutachtet. ☒ ***Übertragungs- und Weitergabekontrolle*** *(Überprüfung, an welche Stellen personenbezogene Daten übermittelt wurden)*

	Alle Datenübertragungen über das Internet im Zusammenhang mit AV1 sind mindestens nach dem Standard TLS 1.2 verschlüsselt und decken die für die Dienste erforderlichen Übertragungen ab. Alle Signale werden mit starken Schlüsseln verschlüsselt und verwenden das HTTPS-Protokoll. Datenbanken/Server haben verschlüsselte Festplatten/Backups/Kommunikation. Der gesamte Medienverkehr (d. h. Audio- und Videostreams) verwendet SRTP (mit DTLS für den Schlüsselaustausch) oder DTLS. Die Kommunikation wird Ende-zu-Ende mit diesen Schlüsseln unter Verwendung von SRTP verschlüsselt, unabhängig davon, ob die Kommunikation direkt zwischen dem AV1 und den Anwendungen oder über ein Relais erfolgt.) Die für den Verbindungsaufbau erforderlichen Metadaten (einschließlich IP-Adresse, Endpunktkennungen und Verschlüsselungsschlüssel) werden mit TLS verschlüsselt zwischen AV1 und den Servern von No Isolation übertragen. Für den Aufbau des Audio- und Videostroms wird der WebRTC-Standard verwendet, und die WebRTC-Signale (d. h. die Metadaten) werden (TLS-verschlüsselt) über die No-Isolation-Server übertragen.
Maßnahmen zur Gewährleistung der **Verfügbarkeit** personenbezogener Daten und des raschen Zugangs zu Daten im Falle eines physischen oder technischen Zwischenfalls	☒ Wiederherstellbarkeit (Recovery / Backup) No Isolation nutzt Cloud-Dienste, um sicherzustellen, dass Daten und Dienste im Bedarfsfall verfügbar sind. Der Anbieter erstellt alle 24 Stunden Sicherungskopien kritischer Systeme. Die Backups werden in der Cloud gespeichert, damit die Systeme bei Bedarf schnell an einem anderen Ort wiederhergestellt werden können (z. B. bei Schäden wie Feuer oder Stromausfällen). No Isolation unterhält einen Geschäftskontinuitätsplan ("BC-Plan"), der Verfahren zum Schutz vor Unterbrechungen durch unerwartete Ereignisse vorsieht und Meldewege, Notfallkontakte, die Bildung von Reaktionsteams und Notfallpläne für kritische Systeme umfasst. Der BC-Plan wird jährlich getestet, wobei die Ergebnisse und Verbesserungen im Rahmen des Informationssicherheitsmanagementsystems von No Isolation verwaltet werden. Software- und Konfigurationsinformationen, die sich auf die Systeme und die intern entwickelten und verwalteten Anwendungsdienste beziehen, werden in einem sicheren Quellcode-Repository verwaltet. No Isolation kann Anwendungsdienste bei Bedarf schnell wiederherstellen oder neu bereitstellen. Dazu gehört auch die Möglichkeit, die Dienste bei Bedarf an einen anderen Standort zu verlagern.

	☒ Zuverlässigkeitskontrolle (Meldung von Fehlfunktionen, Störungen und Gefahren) Vernetzte Systeme sind durch Firewalls, Endpoint-Protection-Dienste, Überwachungs- und Verwaltungstools gegen unbefugtes Eindringen gesichert. Die Infrastruktur von No Isolation protokolliert Informationen über das Systemverhalten, den empfangenen Datenverkehr, die Systemauthentifizierung und andere Anwendungsanfragen. Interne Systeme warnen die zuständigen Mitarbeiter vor böswilligen, unbeabsichtigten oder untypischen Aktivitäten. Das Personal von No Isolation, einschließlich des Sicherheitspersonals, des Betriebspersonals und des Supportpersonals, wird geschult, um auf erkannte Sicherheitsvorfälle zu reagieren. Über erkannte Sicherheitsvorfälle werden Aufzeichnungen geführt. Verdächtige und bestätigte Sicherheitsvorfälle werden untersucht und die entsprechenden Lösungsschritte werden dokumentiert. Bei bestätigten Sicherheitsvorfällen wird eine Überprüfung nach dem Sicherheitsvorfall durchgeführt und es werden geeignete Maßnahmen ergriffen, um das Risiko eines Schadens oder einer unbefugten Offenlegung zu minimieren. Der Dienstleister überwacht seine Systeme kontinuierlich und benachrichtigt das Betriebspersonal direkt, wenn ein System ausfällt. Überwachungsanwendungen werden eingesetzt und konfiguriert, um die Systemkapazität zu überwachen und das Betriebspersonal zu alarmieren, wenn vordefinierte Schwellenwerte erreicht werden. ☒ Verfügbarkeit (Redundanzen der Systeme und Infrastrukturen) Die Routinen für die Geschäftskontinuität, die Notfallwiederherstellung und die Reaktion auf Zwischenfälle werden vom Cloud-Infrastruktur-Anbieter und den SaaS-Anbietern von No Isolation bereitgestellt (die wirtschaftlich angemessene Anstrengungen unternehmen, um Betriebszeit, redundante Stromversorgung, Netzwerk und HLK-Dienste zu gewährleisten). ISO 27001-Richtlinien, z. B. für Schwachstellenmanagement, Datensicherung, Risikomanagement, Patch-Management, zeigen einen verwalteten Ansatz für die Ziele der Informationssicherheit. Die Infrastruktur wird von AWS mit getrennten Umgebungen für Entwurf/Test (Staging) und Produktion bereitgestellt. Die Verfügbarkeit wird ständig überwacht.

Gewährleistung, dass personenbezogene Daten, entsprechend den **Weisungen des Auftraggebers** und **getrennt nach den entsprechenden Zwecken** verarbeitet werden	☒ **Auftragskontrolle** (personenbezogene Daten werden nur entsprechend den Weisungen des Auftraggebers verarbeitet) No Isolation hat mit seinem Personal (einschließlich Angestellten, Beratern und externen Vertragspartnern) Verträge abgeschlossen, die Vertraulichkeitsverpflichtungen beinhalten. Die Verpflichtung zur Vertraulichkeit besteht auch nach Beendigung des Arbeitsverhältnisses und solange die Informationen vertraulich bleiben. Der Zugang zur Ferndiagnose wird nur nach Genehmigung durch den Kunden gewährt. Ferndiagnosesitzungen werden protokolliert, und je nach erforderlicher Zugriffsstufe muss das Supportpersonal einen physischen Hardware-Authentifizierungsschlüssel vorlegen, um die Ferndiagnosesitzung zu starten. No Isolation ist über einen AV-Vertrag verpflichtet, Daten nur auf dokumentierte Weisung zu verarbeiten. Das Personal wird entsprechend informiert und geschult. Es ist festgelegt, welche Personen Weisungen zur Verarbeitung erteilen und entgegennehmen dürfen. ☒ Datentrennbarkeit (zu unterschiedlichen Zwecken erhobene personenbezogene Daten werden getrennt verarbeitet) Eine zusätzliche logische Trennung wird innerhalb der Software von No Isolation durch feste und eindeutige Kunden- und Gerätekennungen und sichere temporäre sitzungsbasierte Token durchgesetzt, die bei erfolgreich authentifizierten Verbindungen erzeugt werden.
Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung der **Wirksamkeit der technischen und organisatorischen Maßnahmen** zur Gewährleistung der Sicherheit der Verarbeitung	☐ Ein(e) Datenschutzbeauftragte(r) (DSB) ist benannt ☒ Ein Informationssicherheitsbeauftragter (ISB) ist bestellt ☐ Privacy Information Management System (PIMS) ☒ Information Security Management System (ISMS)
Nachweise über die Sicherheit der Datenverarbeitung auf Basis von Zertifizierungen oder anerkannter organisatorischer Maßnahmen	**Zertifizierungen der Informationssicherheit:** ☒ ISO 27001 – Information Security Management System ☐ ISO 27017 – Information Security controls for cloud services ☐ ISO 27018 – Protection of personally identifiable information (PII) in public clouds

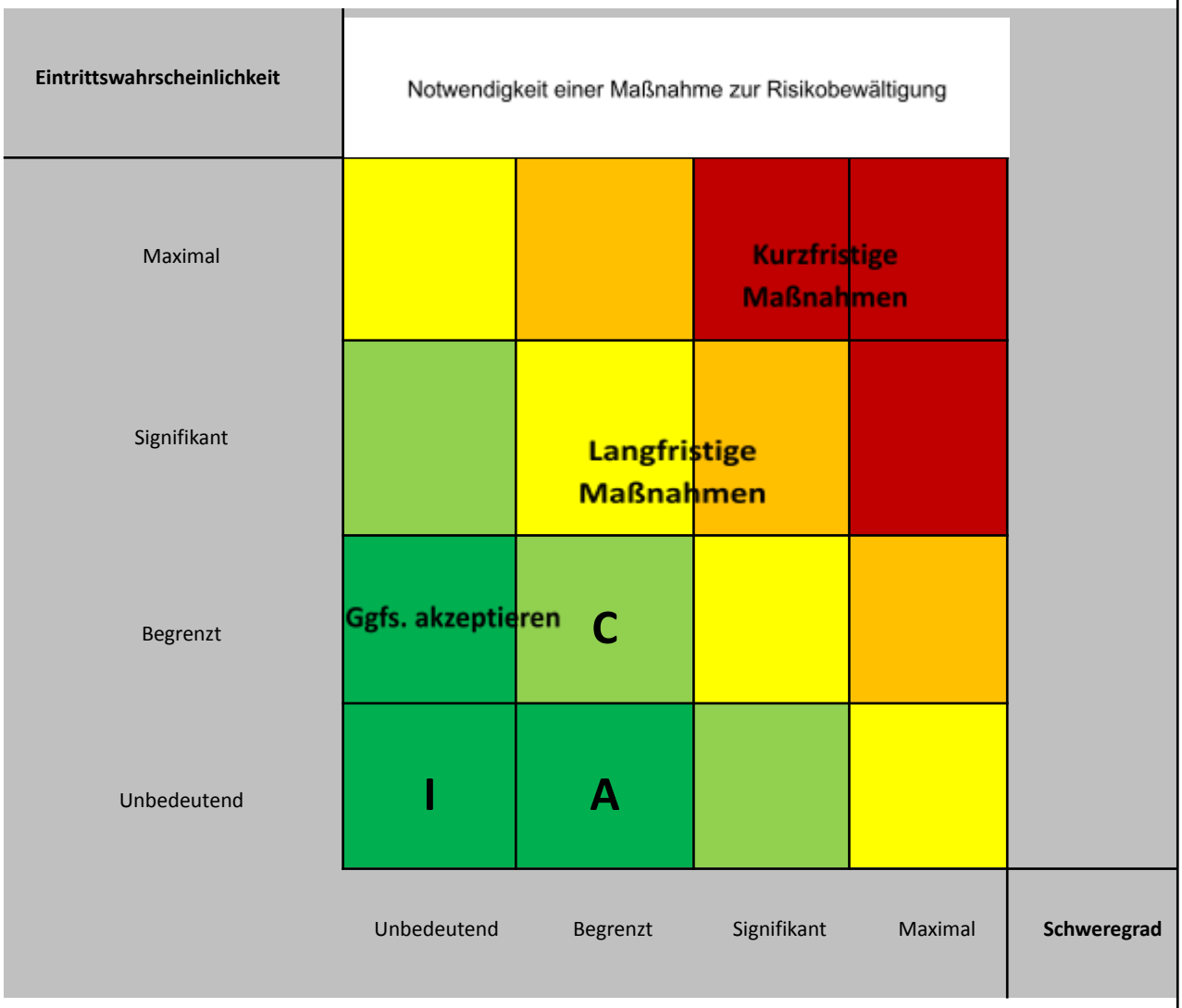
	☐ ISO 27701 - Privacy information management ☐ IT-Grundschutz based on ISO 27001 (BSI) ☐ TISAX (ENX) Als führender Cloud-Anbieter verfügt der Unterauftragnehmer AWS auch über mehrere Zertifizierungen, z. B. ISO 27001 und SOC2. *Recognized organisational measures* ☐ Approved Binding Corporate Rules (BCR)

Bemerkung: Die Angaben zu den Kontrollen sind durch dokumentierte Konzepte und Richtlinien im Rahmen der ISO 27001-Zertifizierung glaubwürdig nachprüfbar

7 Bewertung der Risiken für die Datenverarbeitung unter Berücksichtigung der TOMs nach Art. 32 DSGVO

Verlust der **Vertraulichkeit**:	Verlust der **Integrität**	Verlust der **Verfügbarkeit**
☐ maximal ☐ signifikant ☒ begrenzt ☐ unbedeutend **C**	☐ maximal ☐ signifikant ☐ begrenzt ☒ unbedeutend **I**	☐ maximal ☐ signifikant ☐ begrenzt ☒ unbedeutend **A**

Betroffenenrisiko	**Organisationsrisiko**	**Fazit:**
☐ maximal ☐ signifikant ☒ begrenzt ☐ unbedeutend	☐ maximal ☐ signifikant ☒ begrenzt ☐ unbedeutend	Nach der durchgeführten Risikobewertung und unter Berücksichtigung einer möglichen Datenübermittlung an Drittländer ergibt sich aus der Datenverarbeitung mit AV1 ein begrenztes Risiko für die betroffenen Personen.



msecure GmbH
Bajuwarenring 21
82041 Oberhaching